Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) ~~In a network device having a plurality of ports and providing routing functionality between ports, a~~ A method ~~for providing security,~~ comprising:

identifying, by a network device, ~~at least~~ a first port of [[a]] the network device as a management port, the first port having a ~~first~~ gateway address~~, as being a management port~~;

identifying, by the network device, a ~~group of ports~~ second port of the network device as ~~being~~ a non-management ~~ports~~ port; and

filtering, by the network device, [[out]] management data packets received on ~~any of the non-management ports~~ the second port.

2. (Currently Amended) The method of claim 1, ~~further~~ wherein the filtering ~~out management data packets~~ includes:

determining if a destination IP address for a data packet received on ~~one of the group of non-management ports~~ the second port has a destination IP address ~~which~~ that corresponds to the gateway address of the first port.

3. (Currently Amended) The method of claim 2, wherein the filtering ~~out management data packets~~ further includes:

if the destination IP address for the data packet received on the second port corresponds to the gateway address of the first port, determining if [[a]] the data packet ~~received on one of the group of ports~~ utilizes a management protocol; and

if the data packet utilizes a management protocol, dropping [[a]] the data packet ~~where it is determined that a data packet received on one of the group of ports has a destination IP address which corresponds to the gateway address of the first port, and that the data packet utilizes a management protocol~~.

Appl. No. 10/668,455
Amdt. dated June 18, 2009
Reply to Office Action of March 20, 2009

PATENT

4.   (Currently Amended) The method of claim 1, further comprising:

defining a virtual local area network ~~to include~~ including the first port[[,]] and ~~to include~~ a first ~~layer 2~~ subnet; and

allowing access to management functions of the network device only to those hosts ~~which are~~ connected to the first ~~layer 2~~ subnet.

5.   (Currently Amended) The method of claim [[1]] 4, further comprising:

~~defining a virtual local area network to include the first port, and to include a first layer 2 subnet;~~

~~allowing access to management functions of the network device only to those hosts which are connected to the first layer 2 subnet;~~

connecting ~~a first layer 2 switch~~ another network device to [[a]] the second port ~~of the group of ports~~;

defining a ~~plane~~ port of the ~~layer 2 device to be~~ another network device as part of the virtual local area network, wherein the ~~plane~~ port of the ~~layer 2 device~~ another network device is assigned a source IP address ~~which~~ that corresponds to the gateway address of the first port~~,; and~~ and wherein [[all]] management data packets for managing the ~~first layer 2 device~~ another network device are sent to the source IP address ~~which is assigned to the plane of the layer 2 device is part of the virtual local area network~~.

6.   (Currently Amended) The method of claim 5, wherein [[all]] management ~~commands~~ data packets have higher priority than [[all]] other data packets routed through the network device.

7.   (Currently Amended) The method of claim 1, further including:

providing an application specific integrated circuit ~~which is~~ operable to filter ~~out all~~ management data packets received on ~~any of the non-management ports~~ the second port.

8.   (Currently Amended) The method of claim 1 further including:

providing an application specific integrated circuit ~~which is~~ operable to:

Appl. No. 10/668,455
Amdt. dated June 18, 2009
Reply to Office Action of March 20, 2009

PATENT

determine if a destination IP address for a data packet received on ~~one of the group of non-management ports is a destination IP address which~~ the second port corresponds to the gateway address of the first port~~;, and to~~

determine if [[a]] the data packet ~~received on one of the first group of ports~~ utilizes a management protocol~~;~~[[,]] and [[to]]

drop [[a]] the data packet ~~where~~ if it is determined that [[a]] the data packet ~~received on one of the group of ports~~ has a destination IP address ~~which~~ that corresponds to the gateway address of the first port, and that the data packet utilizes a management protocol.

9.   (Currently Amended) A network device ~~for routing data packets, the network device including~~ comprising:

a first port ~~which is~~ defined ~~to be~~ as a management port;

a ~~group of ports~~ second port ~~which are not management ports~~ defined as a non-management port;

a ~~CPU which is~~ processing component operable to provide management functions~~,~~ ~~which~~ that allow a user to modify [[the]] operation of the network device; and

an application specific integrated circuit ~~which is~~ operable to deny access to the [[CPU]] management functions for [[all]] hosts ~~which~~ that transmit management data packets to the network device through ~~any of the group of ports~~ the second port.

10.   (Currently Amended) The network device of claim 9~~, wherein:~~

~~the first port has a first gateway IP address;~~

wherein the application specific integrated circuit ~~receives data packets, received on each port of the group of ports, and~~ is further operable to~~:~~

determine if a data packet received on [[one]] the ~~group of ports contains~~ second port includes a destination IP address ~~which~~ that corresponds to ~~the first~~ a gateway IP address of the first port~~;~~

~~wherein the application specific integrated circuit is further operable to~~ if the destination IP address corresponds to the gateway IP address, determine if [[a]] the data packet ~~received on one of the group of ports~~ utilizes a management protocol; and

if the data packet utilizes a management protocol, ~~wherein when it is determined that a data packet received on one of the group of ports is directed to a destination IP address which corresponds to the first gateway IP address and is in a management protocol, the application specific integrated circuit operates to~~ drop the data packet.

11.   (Currently Amended) The network device of claim 10, wherein the first port is defined to be part of a management virtual local area network, and <u>wherein</u> only devices <u>that</u> are coupled to the management virtual <u>local</u> area network have access to the management functions of the [[CPU]] <u>processing component</u>.

12.   (New) A network device comprising:

a plurality of ports including a management port; and

a control component configured to:

determine if a destination IP address included in a received data packet corresponds to a gateway IP address of the management port;

if the destination IP address does not correspond to the gateway IP address of the management port, determine if the data packet originated from a management virtual local area network (VLAN), wherein the management VLAN includes the management port;

if the destination IP address did not originate from the management VLAN, determine if the data packet uses a management protocol; and

if the data packet uses a management protocol, drop the packet.

13.   (New) The network device of claim 12 wherein if the destination IP address does correspond to the gateway IP address of the management port, the control component is configured to pass the data packet.

14.   (New) The network device of claim 12 wherein if the destination IP address did originate from the management VLAN, the control component is configured to pass the data packet.

15.   (New) The network device of claim 12 wherein if the data packet does not use a management protocol, the control component is configured to pass the data packet.

16.   (New) The network device of claim 12 wherein the network device is a router.